DEPARTMENT OF JUSTICE

JOSEPH R. BIDEN, III
ATTORNEY GENERAL

820 NORTH FRENCH STREET
WILMINGTON, DELAWARE 19801

PHONE (302) 577-8338
FAX (302) 577-2601

PHISHING

Criminals use a variety of techniques to steal your confidential personal and financial information. "Phishing" is one of those techniques. Protect yourself from identity theft by learning to recognize Phishing and other scams that gather your private and confidential information for criminal purposes**.**

What is Phishing?

• Phishing is a crime that uses the telephone, email or computer pop-ups to steal your personal information for illegal purposes.

• Phishers pretend to be legitimate businesses that you may already deal with, such as a bank or credit card company, your Internet service provider, or even the government.

• Phishing messages look official and legitimate and can fool unsuspecting people.

• Phishers give a legitimate-sounding reason for why you should give them social security numbers, birth dates, credit card and bank account numbers and other personal and confidential information.

• Phishers often threaten to close your account if you refuse to give them your information.

How do I know I'm being "Phished"?

• If you're asked to provide confidential information by phone, tell the caller you will not give them the information and hang up. Don't call any number given to you by the caller; it may be part of the scam. Look up the company's number your self and call to determine if the call was legitimate.

• Every time you're asked to click on a link in an email to provide confidential information, you are dealing with a criminal phisher. Never click on such links and delete the email message immediately. Legitimate companies never ask for this type of information in an email as email is not secure.

How else can I protect myself from Phishing?

• Delete computer messages that ask for confidential information – don't open attachments or click on links

• Never email personal or confidential information. Email is not secure.

• Regularly update your anti-virus and anti-spyware software

• Install a firewall to protect your computer.

• Type web addresses into browsers – never click on a link in an unsolicited email.

• Change your passwords and PINS regularly.

• Review all credit card statements monthly for unauthorized charges and report any charges immediately.

• Regularly review your credit reports from the three major credit bureaus.

• If you receive a "phishing" email, forward it to the Federal Trade Commission at uce@ftc.gov.

What should I do if I'm hooked by a Phisher?

• Report the theft to your local police department. Immediately alerting local law enforcement to the crime may help locate the thief and stop others from being victimized. Reporting gives you proof that you acted diligently and provides you with a police report, complaint number or similar record that may be required by your creditors.

• Contact The Attorney General's Consumer Protection Unit at (800) 220-5424 to obtain the Identity Theft Victim Kit which guides you step by step on what you need to do to report and document the incident. The Kit is also available on the Attorney General's website at www.state.de.us/attgen/

• Report the theft to the three major credit bureaus and ask them to place a "fraud alert" on your credit report. Order your credit report and review it carefully for any authorized credit activity. Give the credit bureaus your file or complaint number from the police report and any other information they may need. The three major credit bureaus are:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834-6790
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 680-7289

• Gather all of your credit card, bank account and other creditor information (such as utilities, cable, etc.). Contact the fraud departments of each creditor and ask that a "fraud alert" be placed on your account. If there are illegal charges on your accounts, most creditors will ask you to submit a written report of the fraud, along with a police report, or police complaint number or file number.

• Report the theft to the Federal Trade Commission ("FTC") which maintains a confidential, national Identity Theft database, and may also be able to assist in pursuing identity thieves through federal channels. You can reach the FTC toll-free at 1-877-438-4338. The TTY line for the hearing impaired is 1-866-653-4261. The website for the FTC is www.ftc.gov